Annex A

Compliance Criteria
Computer Security Incident Management

Cross-Reference: Compliance Criteria Referenced to NIST Information Systems Security Guidelines

This page intentionally blank.

Table of Contents

Annex Overview

This annex is published in support of the **Statewide Standard: Computer Security Incident Management** (Standard), and provides compliance criteria for the security controls derived from NIST Special publications.

Within this annex, the term "organization" refers to organizations or parties subject to the Standard.

I. Baseline Controls

Baseline controls are the minimum security controls recommended for an information system based on the system's security categorization in accordance with FIPS PUB 199 - Standards for Security Categorization of Federal Information and Information Systems.

The tailored security control baseline serves as the starting point for organizations in determining the appropriate safeguards and countermeasures necessary to protect their information systems. Because the baselines are intended to be broadly applicable starting points, subsequent supplements to the tailored baselines will likely be necessary in order to achieve ongoing adequate risk mitigation as the organizations' risk environment changes. Reference the NIST Special Publications for detailed guidance.

The tailored baselines are supplemented based on organizational assessments of risk (i.e., a risk assessment) and the resulting controls documented in the security plans for the information systems.

Reference the National Institutue of Science and Technology (NIST) Special Publication (SP) 800-53 Revision 2 Recommended Security Controls for Federal Information Systems for further guidance on controls.

II. NIST Special Publications

The NIST publications specify both recommendations and requirements. However, for compliance purposes this annex applies NIST Special Publications content as specific "general", "control" and "control enhancement" requirements of the Standard, which are to be implemented based upon the policy requirements. Reference the Standard.

Reference the NIST Special Publications for details of the requirements and further implementation guidance.

III. NIST Baseline Controls Quick-Reference Table

The following table depicts the controls required based on impact. Reference FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems for guidance and specifications defining "low", "moderate", and "high" impacts.

Label	Control Name	Low-Impact	Moderate-Impact	High-Impact
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	Not Selected	IR-2	IR-2 (1)
IR-3	Incident Response Testing and Exercises	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	Not Selected	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)

Notes: "Not Selected" means not required for that impact category.

Numbers in parentheses indicate "control enhancements" required beyond the basic control.

Compliance Specifications

IV. General Compliance Criteria

Compliance shall be attained through development of the general controls which are the foundation supporting the implementation of the additional "low-", "moderate-", or "high-" impact baseline controls.

The following are compliance indicators of the general control requirements of the Standard, applicable to all baseline implementations:

To achieve compliance with the Standard, the organization has:

1. Implemented the "general controls" as referenced in this annex as a foundation control set, documented in paragraph **IV. General Compliance Criteria,** et seq; **and**

    a. Implemented the appropriate "impact baseline" controls based upon an assessment of their data and information assets, the state of their information systems, and the vulnerabilities and risk posed to those assets,

    Or…

    b. Without an assessment, implemented the level of controls based upon the schedule requirements of the Standard.

Regardless of implementation strategy above, the organization has selected security controls appropriate for the protection of those assets based upon the impact baseline, and the level of acceptable risk based upon the following:

- For general controls applicable to all baselines: NIST SP800-61 Revision 1.
- For controls applicable to *Low-Impact Baseline*: NIST SP800-53 Recommended Security Controls for Federal Information Systems (latest revision), Annex 1, Low-Impact Baseline incident response (IR) family (**Annex 1**).
- For controls applicable to *Moderate-Impact Baseline*: NIST SP800-53 Recommended Security Controls for Federal Information Systems (latest revision), Annex 2, Moderate-Impact Baseline incident response (IR) family (**Annex 2**).
- For controls applicable to *High-Impact Baseline*: NIST SP800-53 Recommended Security Controls for Federal Information Systems (latest revision), Annex 3, High-Impact Baseline incident response (IR) family (**Annex 3**).

The content of these publications form the basis of compliance, as documented in subsequent paragraphs.

A. Incident Response Plan

Reference: NIST SP800-61 Revision 1, Paragraph 2.3.2 and 2.6

Control: The organization has published an incident response plan to provide a roadmap for implementing an incident response program based on the Policy. The plan indicates both short- and long-term goals for the program, including metrics for measuring the program. The incident response plan indicates how often incident handlers shall be trained and the requirements for incident handlers.

B. Incident-Related Information Sharing

Reference: NIST SP800-61 Revision 1, Paragraph 2.3.4 and 2.6

Control: The organization communicates incident details with outside parties as required, such as the media, law enforcement agencies, and incident reporting organizations. The incident response team has discussed this requirement at length with the organization's public affairs office, legal department, and management; and has established policies and procedures regarding information sharing. The team complies with existing organization policy on interacting with the media and other outside parties.

C. Incident Response Team Model

Reference: NIST SP800-61 Revision 1, Paragraph 2.4.1, 2.4.2 and 2.6

Control: The organization carefully weighs the advantages and disadvantages of each possible team structure model and staffing model in the context of the organization's needs and available resources; and has determined and implemented an appropriate model.

D. Select the Incident Response Team

Reference: NIST SP800-61 Revision 1, Paragraph 2.4 and 2.6

Control: The organization ensures personnel included on the Incident Response Team have appropriate technical and communication skills and are proficient in the context of incident response.

The credibility and proficiency of the team depend to a large extent on the technical skills of its members. Poor technical judgment can undermine the team's credibility and cause incidents to worsen. Critical technical skills include system administration, network administration, programming, technical support, and intrusion detection. Teamwork and communications skills are also needed for effective incident handling.

E. Additional Service

Reference: NIST SP800-61 Revision 1, Paragraph 2.5

Control: The organization performs additional security-related functions as required by incident response measures, including distributing security advisories, performing vulnerability assessments, educating users on security, and monitoring intrusion detection sensors.

F. Evaluate Incident Response Program

Control: The organization evaluates the incident response program annually, to include testing and exercising the complete program.

G. Incident Response Policy and Procedures

Reference: NIST SP800-61 Revision 1, Paragraph 2.3 and 2.6

Control: The organization develops, disseminates, and periodically reviews and/update: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

1. IR-1 Incident Response Procedures

Reference: NIST SP800-53, Revision 2, Annex 3: High-Impact Baseline, Family: Incident Response

Control: The organization publishes incident response procedures to provide detailed steps for responding to an incident based on NIST SP800-61, the incident response policy; and conform to this Standard, and the incident response plan.

Control Enhancements: None.

V. Ratings of Incidents

Rating, categorizing or classifying incidents is accomplished in compliance to the State of Montana Continuity of Government (COG) plans, policies, and standards, and the prioritization of computer security incidents occurs within overall COG requirements.

A. Prioritization or Severity

Reference: NIST SP800-61 Revision 1, Paragraph 3.2.6

Control: Incidents are prioritized based on two factors:

1. Current and Potential Technical Effect of the Incident

Incident handlers consider not only the current negative technical effect of the incident (e.g., unauthorized user-level access to data), but also the likely future technical effect of the incident if it is not immediately contained (e.g., root compromise). For example, a worm spreading among workstations may currently cause a minor effect on the agency, but within a few hours the worm traffic may cause a major network outage.

2. Criticality of the Affected Resources

Resources affected by an incident (e.g., firewalls, Web servers, Internet connectivity, user workstations, and applications) have different significance to the organization. The criticality of a resource is based primarily on its data or services, users, trust relationships and interdependencies with other resources, and visibility (e.g., a public Web server versus an internal department Web server). When possible, the incident response team shall acquire and reuse existing valid data on resource criticality.

VI. Performance Measures

Control: The Incident Management Plan includes metrics to support program, plan and procedure evaluation. Metrics include:

A. Number of Incidents Handled

1. Handling multiple incidents.

For example, the number of incidents handled may decrease because of better network and host security controls, not because of negligence by the incident response team. The number of incidents handled is best taken as a measure of the relative amount of work that the incident response team had to perform, not as a measure of the quality of the team, unless it is considered in the context of other measures that collectively give an indication of work quality. It is more effective to produce separate incident counts for each incident category (e.g., unauthorized access).

1. Subcategories used to provide more information.

For example, a growing number of unauthorized access incidents performed by insiders could prompt stronger policy provisions concerning background investigations for personnel and misuse of computing resources and stronger security controls on internal networks (e.g., deploying intrusion detection software to more internal networks and hosts).

B. Time per Incident

Control: For each incident, time is measured in several ways:

- Total amount of labor spent working on the incident
- Elapsed time from the beginning of the incident to its resolution

- Elapsed time for each stage of the incident handling process (e.g., containment, recovery)
- How long it took the incident response team to respond to the initial report of the incident.
- How long it took to report the incident to management and, if necessary, appropriate external entities (e.g., US-CERT).

C. Objective Assessment of Each Incident

Control: The response to each incident is analyzed to determine the effectiveness of the response. The following are examples of performing an objective assessment of an incident:

- Reviewing logs, forms, reports, and other incident documentation for adherence to established incident response policies and procedures
- Identifying which precursors and indications of the incident were recorded to determine how effectively the incident was logged
- Determining if the incident caused damage before it was detected
- Determining if the actual cause of the incident was identified
- Calculating the estimated monetary damage from the incident
- Identifying which measures, if any, could have prevented the incident.

D. Subjective Assessment of Each Incident

Control: Incident response team members assess their own performance, as well as that of other team members and of the entire team. Another valuable source of input is the owner of a resource that was attacked—to determine if the owner believes the incident was handled efficiently and if the outcome was satisfactory.

VII. Reporting

A. Requirements

Reference: NIST SP800-61 Revision 1, Paragraph 2.6

Control: The Incident Response Plan includes provisions concerning incident reporting—at a minimum, what must be reported to whom and at what times (e.g., initial notification, regular status updates), including:

- When an incident is analyzed and prioritized, the incident response team shall notify the appropriate individuals within the organization and, as required, other organizations.
- Timely reporting and notification to enable those who need to be involved to engage effectively.

1. Incident Reporting Organizations

Reference: NIST SP800-61 Revision 1, Paragraph 2.3.4.3 and 2.6

Control: The organization promptly reports incident information to appropriate authorities and to the common and central incident management function provided by the Department of Administration.

Low-Impact Baseline Controls

VIII. Requirements and Specifications – Low-Impact

The following are compliance indicators of the Standard for low-impact baseline implementations:

A. IR-2 Incident Response Training

No compliance required.

B. IR-3 Incident Response Testing and Exercises

No compliance required.

C. IR-4 Incident Handling

Reference: NIST SP800-53, Revision 2, Annex 1: Low-Impact Baseline, Family: Incident Response ***(Annex 1)***

Control: The organization has implemented an incident handling capability for security incidents that includes preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity.

Control: The organization has implemented the guidance of NIST SP800-61 chapters three through eight into procedures.

Control Enhancements: No compliance required.

D. IR-5 Incident Monitoring

No compliance required.

E. IR-6 Incident Reporting

Reference: NIST SP800-53, Revision 2, Annex 1: Low-Impact Baseline, Family: Incident Response ***(Annex 1)***

Control: The organization promptly reports incident information to appropriate authorities and to the common and central incident management function provided by the Department of Administration.

Control Enhancements: No compliance required.

F. IR-7 Incident Response Assistance

Reference: NIST SP800-53, Revision 2, Annex 1: Low-Impact Baseline, Family: Incident Response ***(Annex 1)***

Control: The organization provides an incident response support resource(s) that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource(s) are an integral part of the organization's incident response capability.

Control Enhancements: No compliance required.

1. Incident Handling Participation

Reference: NIST SP800-61 Revision 1, Paragraph 2.4.3 and 2.6

Control: The organization includes incident response team members based on the expertise, judgment, and abilities of core and supporting functions, including management, information security, IT support, legal, public affairs, and facilities management.

End of Low-Impact Cross-Reference

Moderate-Impact Baseline Controls

IX. Requirements and Specifications – Moderate-Impact

The following are compliance indicators of the Standard for moderate-impact baseline implementations:

A. IR-2 Incident Response Training

Reference: NIST SP800-53, Revision 2, Annex 2: Moderate-Impact Baseline, Family: Incident Response ***(Annex 2)****, and NIST SP800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*

Control: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provide refresher training at least annually.

Control Enhancements: No compliance required.

B. IR-3 Incident Response Testing and Exercises

Reference: NIST SP800-53, Revision 2, Annex 2: Moderate-Impact Baseline, Family: Incident Response ***(Annex 2)****, and NIST SP800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*

Control: The organization tests and/or exercises the incident response capability for the information system at least annually to determine the incident response effectiveness and document the results.

Control Enhancements: No compliance required.

C. IR-4 Incident Handling

Reference: NIST SP800-53, Revision 2, Annex 2: Moderate-Impact Baseline, Family: Incident Response ***(Annex 2)***

Control: The organization has implemented an incident handling capability for security incidents that includes preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity.

Control: The organization has implemented the guidance of NIST SP800-61 chapters three through eight into procedures.

Control Enhancements: The organization employs automated mechanisms to support the incident handling process.

D. IR-5 Incident Monitoring

Reference: NIST SP800-53, Revision 2, Annex 2: Moderate-Impact Baseline, Family: Incident Response ***(Annex 2)***

Control: The organization tracks and documents information system security incidents on an ongoing basis.

Control Enhancements: No compliance required.

E. IR-6 Incident Reporting

Reference: NIST SP800-53, Revision 2, Annex 2: Moderate-Impact Baseline, Family: Incident Response ***(Annex 2)***

Control: The organization promptly reports incident information to appropriate authorities and to the common and central incident management function provided by the Department of Administration.

Control Enhancements: The organization employs automated mechanisms to assist in the reporting of security incidents.

F. IR-7 Incident Response Assistance

Reference: NIST SP800-53, Revision 2, Annex 2: Moderate-Impact Baseline, Family: Incident Response ***(Annex 2)***

Control: The organization provides an incident response support resource(s) that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource(s) are an integral part of the organization's incident response capability.

Control Enhancements: The organization employs automated mechanisms to increase the availability of incident response-related information and support.

1. Incident Handling Participation

Reference: NIST SP800-61 Revision 1, Paragraph 2.4.3 and 2.6

Control: The organization includes incident response team members based on the expertise, judgment, and abilities of core and supporting functions, including management, information security, IT support, legal, public affairs, and facilities management.

End of Moderate-Impact Cross-Reference

High-Impact Baseline Controls

X. Requirements and Specifications – High-Impact

The following are compliance indicators of the Standard for high-impact baseline implementations:

A. IR-2 Incident Response Training

Reference: NIST SP800-53, Revision 2, Annex 3: High-Impact Baseline, Family: Incident Response, and NIST SP800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

Control: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provide refresher training at least annually.

Control Enhancements: The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

B. IR-3 Incident Response Testing and Exercises

Reference: NIST SP800-53, Revision 2, Annex 3: High-Impact Baseline, Family: Incident Response, and NIST SP800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

Control: The organization tests and/or exercises the incident response capability for the information system at least annually to determine the incident response effectiveness and document the results.

Control Enhancements: The organization employs automated mechanisms to more thoroughly and effectively test and exercise the incident response capability.

C. IR-4 Incident Handling

Reference: NIST SP800-53, Revision 2, Annex 3: High-Impact Baseline, Family: Incident Response

Control: The organization has implemented an incident handling capability for security incidents that includes preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity.

Control: The organization has implemented the guidance of NIST SP800-61 chapters three through eight into procedures.

Control Enhancements: The organization employs automated mechanisms to support the incident handling process.

D. IR-5 Incident Monitoring

Reference: NIST SP800-53, Revision 2, Annex 3: High-Impact Baseline, Family: Incident Response

Control: The organization tracks and documents information system security incidents on an ongoing basis.

Control Enhancements: The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

E. IR-6 Incident Reporting

Reference: NIST SP800-53, Revision 2, Annex 3: High-Impact Baseline, Family: Incident Response

Control: The organization promptly reports incident information to appropriate authorities and to the common and central incident management function provided by the Department of Administration.

Control Enhancements: The organization employs automated mechanisms to assist in the reporting of security incidents.

F. IR-7 Incident Response Assistance

Reference: NIST SP800-53, Revision 2, Annex 3: High-Impact Baseline, Family: Incident Response

Control: The organization provides an incident response support resource(s) that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource(s) are an integral part of the organization's incident response capability.

Control Enhancements: The organization employs automated mechanisms to increase the availability of incident response-related information and support.

1. Incident Handling Participation

Reference: NIST SP800-61 Revision 1, Paragraph 2.4.3 and 2.6

Control: The organization includes incident response team members based on the expertise, judgment, and abilities of core and supporting functions, including

management, information security, IT support, legal, public affairs, and facilities management.

End of High-Impact Cross-Reference

XI. Administrative Use

Document ID:	COMPL-20080715a
Proponent:	Chief Information Officer
Version:	**1.0**.2
Version Date:	2/17/2009
Approved Date:	TBD
Effective Date:	September 1, 2010
Change & Review Contact:	ITSD Service Desk (at http://servicedesk.mt.gov/ess.do)
Review:	Event Review: Any event affecting this architecture paper may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	September 1, 2015
Last Review/Revision:	
Changes:	

End of Annex